# Experimental Demonstration of Free Space Quantum Key Distribution System based on the BB84 Protocol

Adarsh Jain, Abhishek Khanna, Jay Bhatt, Parthkumar V Sakhiya and R K Bahl
Optical Communication Division, Optical & Digital Communication Group,
Satcom & Navigation Payload Area, Space Applications Centre,
Indian Space Research Organization (ISRO), Ahmedabad-380015, INDIA
E-mail:{adarshjain, akn, jay, parthkumar, rkb}@sac.isro.gov.in

***Abstract*— Quantum key distribution (QKD) has emerged as a revolutionary technique that can ensure unconditionally secure communication between two distant parties, referred to as Alice and Bob, by exploiting the fundamental principles of quantum physics. Here, we report experimental demonstration of a fully automated QKD system based on the BB84 protocol. A weak coherent pulse source is developed to generate stream of polarization encoded single photons. Our QKD system demonstrates a low QBER of ~1.2% with sifted key generation rate of ~70 Kbps at an average photon number per pulse of μ = 0.11. The final secure key rate of ~33 Kbps is achieved after performing post processing procedures viz. error correction and privacy amplification. The quantum communication link is established continuously for several hours and the performance is evaluated iteratively. The developed QKD system is shown to have the capability of distributing cryptographic keys securely and seamlessly, under practical operating conditions. Furthermore, we have successfully demonstrated unconditionally secure transmission and reception of an image between Alice and Bob connected over an unsecured public channel by utilizing quantum cryptography.**

***Keywords*—Quantum key distribution (QKD), BB84 protocol, weak coherent pulses, quantum cryptography.**

## I. INTRODUCTION

Recent advancement in quantum computing and quantum information processing technologies creates threat on security of communication systems involving classical cryptographic methods. The security of classical communication may be compromised due to conventional process of key generation or transfer. Hence, modern cryptography deals with challenges lying in efficient and secure distribution of encryption keys to legitimate parties involved in communication. Quantum key distribution (QKD) protocols provide promising solutions for generation and distribution of cryptographic keys to establish unconditionally secure communication between two communicating parties by exploiting the benefits of fundamental principles of quantum physics such as no cloning theorem, indistinguishable nature of photons from a single photon source etc.

Multiple QKD protocols have been proposed so far. The BB84 is very first QKD protocol [1] that exploits virtues of no-cloning theorem and Heisenberg's uncertainty principle to exchange polarization encoded single-photons for generation of a secure key between two parties [2]. BB84 uses quantum properties in an efficient manner and remains the most widely applied protocol for several practical QKD experiments. Other protocols include B92, Decoy state BB84 protocol, SARG04 etc. [3]. The entangled photon pair based protocols such as E91 [4], BBM92 [5] etc. have also been realized.

Free-space and optical fiber are two mode of communication channel for implementing photon based QKD systems [6] [7]. However, the loss of photons in quantum channel due to atmospheric losses or absorption in fiber cables limits the ground based quantum communication to few hundreds of kilometers [7]. To alleviate this problem, satellite based space to ground quantum communication links [8] can be employed with the capability of quantum key distribution between two ground stations located thousands of kilometers apart from each other. Recently, China [9] and Japan [10] have successfully established a quantum communication link from satellite to ground and thereby paved the way for a global scale QKD network.

In this paper, an implementation methodology for a free space QKD system capable of distributing cryptographic keys securely and seamlessly is presented and experimentally demonstrated. The polarization encoded single photon stream is generated by employing weak coherent pulse transmitter. The back-end and front-end software code for complete QKD system is developed, based on BB84 protocol. We have also demonstrated unconditionally secure transmission of an image/text file between two parties connected over an unsecured public channel by exploiting quantum key cryptography.

This paper has been organized as follows. Section II briefly describes the BB84 QKD protocol. In section III, we present the experimental setup for implementing free space quantum key distribution. The software implementation methodology is illustrated in section IV. In section V, the experimental results are presented and discussed. Finally, we conclude and outline the future work in section VI.

## II. BB84 QUANTUM KEY DISTRIBUTION PROTOCOL

In this protocol, two different conjugate bases, '⊕' (represented as rectilinear bases) and '⊗' (represented as diagonal bases) are chosen at random to transmit photons in one of the four $\{|0°\rangle, |90°\rangle, |-45°\rangle, |+45°\rangle\}$ different polarization states. The protocol can be described as per the following three phases:-

### A. *Qubit Transmission*

*1)* Alice first randomly selects a bit value ( i.e. "0" or "1") and also chooses a random basis (i.e. rectilinear: '⊕' basis consisting of polarization states $\{|0°\rangle, |90°\rangle$ or diagonal: '⊗' basis consisting of $\{|-45°\rangle, |+45°\rangle\}$).

*2)* Alice then performs polarization modulation to prepare qubits with a photon in any one of the four quantum states $(|0°\rangle, |90°\rangle, |-45°\rangle, |+45°\rangle)$, and sends them to Bob over the quantum channel.

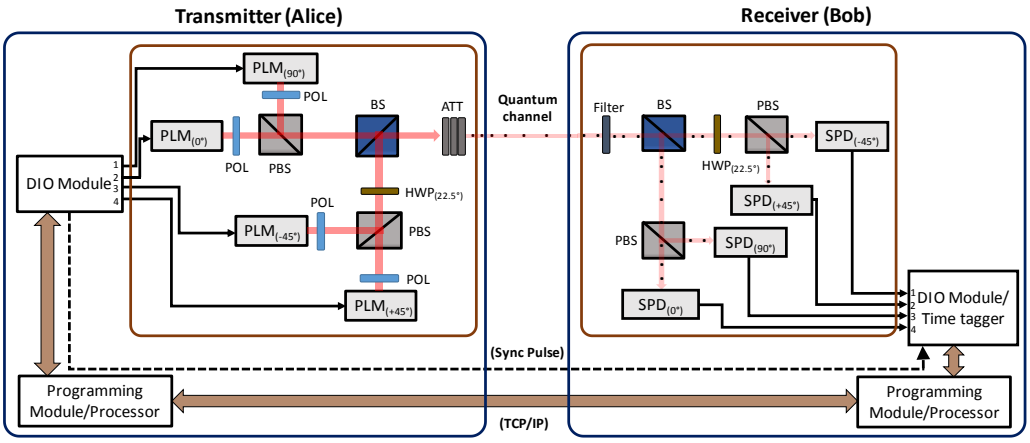


Fig. 1. Block diagram of BB84 protocol based QKD system

*3)* Bob selects a basis, either $\oplus$ or $\otimes$, chosen at random, to measure each of the received qubits. Both, Bob's measurements as well as his choices of bases are recorded.

B. *Key sifting*

*1)* For each bit *Alice* discloses the value of its basis *sends to Bob over the public channel.* Bob responds back to Alice by stating whether he has used the same basis for measurement. Only the bits, where there is an agreement between Alice's prepared and Bob's measured bases are kept while rest are discarded to form the sifted key.

*2)* Alice then discloses to Bob over the public channel, the value of a random subset from the remaining bits. Eavesdropping is then detected by computing quantum bit error rate (QBER).

$$QBER = \#\text{ of incorrect bits/ total shared bits} \quad (1)$$

*3)* The string of bits thus remaining, forms the common secret key Ks.

If an eavesdropper, known as Eve, attempts to listen on the quantum channel by performing a simple intercept-resend attack. In this attack, she first chooses a random basis of measurement and then passes onto Bob a photon with the same polarization state she has just measured; there will be introduction of additional errors and QBER would increase. If Eve, by chance chooses same basis as Alice, Bob receives Alice's state unchanged. However, if she uses incorrect basis, her measurement would end up changing the quantum state. Now, since Bob has equal chance of measuring either of the outcome, the presence of Eve would inadvertently leads to 25% of the key bits being incorrect thereby increasing QBER to ~25%. If such a presence of Eve is detected, the actual data communication over public channel will not be initiated.

C. *Key distillation*

Due to channel and device imperfections, atmospheric turbulence, background noise etc. the received quantum cryptographic key may have some errors. These errors have to be corrected by key reconciliation methods in order to establish a common secret key between the Alice and the Bob. The process should be such that the error correction can be done at receiver side without transmitter declaring any bits on the public channel.

Various standard error correction protocols such as Cascade, Winnow, LDPC etc. can be used for this process [11]. The key reconciliation processes rely on communication between Alice and Bob through the public channel to perform error correction. A procedure, known as privacy amplification [12], is also employed after error correction in order to reduce the amount of leaked information to Eve and to obtain the final secure key.

## III. Experimental Setup

The schematic diagram of our BB84 experimental setup is presented in Fig.1. It consists of a quantum transmitter (Alice) & a quantum receiver (Bob) connected over free space based quantum channel and a TCP/IP link based public channel. The quantum communication link between Alice and Bob has been established, operating over 2 meter of free space optical path.

The quantum transmitter part of the QKD test setup works on the weak coherent pulse based single photon generation technique. The pulse laser module (PLM) emits a train of linearly polarized optical pulses at 785nm wavelength. The two basis set, rectilinear and diagonal, are formed using half wave plate (HWP) and polarization beam splitters (PBS). The polarizers (POL) are placed in front of the PLM to increase the polarization extinction ratio of the incoming beam. The signal from both the basis sets is combined using 50:50 beam splitter (BS). After careful orientation setting and precise alignment, the o/p beam is having any one of the four polarization states i.e. $\{|0°\rangle, |90°\rangle, |-45°\rangle, |+45°\rangle\}$. These laser pulses are then strongly attenuated using a set of neutral density filters (ATT) so as to adjust the average number of photons per pulse ($\mu$) to ~ 0.1. The laser pulses operate at 10 MHz pulse repetition rate and are randomly selected from one of the four laser diodes based on the trigger received from the Tx field programmable gate array (FPGA) DIO module.

The quantum receiver part consists of single photon detector (SPD) modules, passive optical components, FPGA DIO module and time tagging electronics. To cut down the environmental noise levels, the incoming photons are first received using a band pass filter of 5-nm FWHM bandwidth. The incoming photon then passes through a 50:50 beam splitter, which directs it with equal probability, to any one of the two measurement bases i.e. rectilinear $\{|0°\rangle, |90°\rangle\}$ or the diagonal $\{|-45°\rangle, |+45°\rangle\}$. A polarization measurement basis is formed with a HWP and PBS. While the transmitted path functions as the $\{|-45°\rangle, |+45°\rangle\}$ measurement basis $\{|0°\rangle, |90°\rangle\}$ measurement basis is realized using the

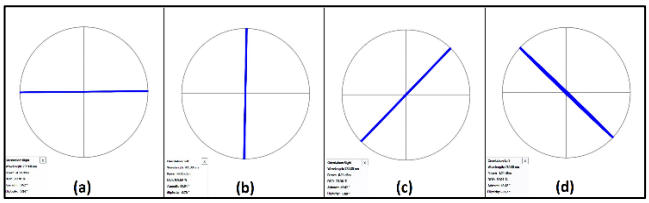


Fig. 2. Measured polarization states (a) $|0°\rangle$ (b) $|90°\rangle$ (c) $|+45°\rangle$ and (d) $|-45°\rangle$

reflected path of BS. For example, a detection click event at $SPD_{(0°)}$ implies projection of the polarization state of the incoming photon to state $|0°\rangle$. All of these Bob's detection events are duly recorded in the Rx FPGA DIO module.

Free space alignment of all the optical components of quantum Tx and Rx setup along with optimization of individual polarization states of the four laser modules was carried out with utmost care to maximize coupling of photons at the Rx side and while minimizing the effects of the optical imperfections on the QBER. The polarization analyzer is used to characterize the polarization states as displayed in Fig.2. The ellipticity of <1.8° and degree of polarization >95% was measured at the Rx side. Free space to fiber couplers are used to couple the incoming stream of photons with the fiber input of SPD modules. The digital output SPD is connected to a PC through Rx FPGA DIO module. The synchronization between Alice and Bob is achieved through TTL sync pulses.

The value of mean photon no. per pulse should be close to 0.1 to get the optical pulses with no photon or only single photon with a very high probability. This is required to achieve provably secure communication and is achieved by optimizing the attenuation value by measuring the count rate at the output of all SPDs. The count rate of ~160K counts/sec/SPD is measured at the Rx side as shown in Fig.3, out of which ~80K counts/sec are due to measurement performed in correct/intended bases and remaining ~80K

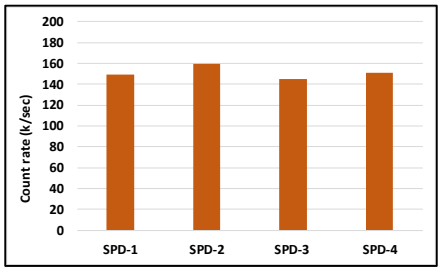


Fig. 3. Measured count rate for SPDs at the Rx side

counts/sec due to measurement in incorrect/unintended bases. This is measured with all four laser modules triggered at a 10 MHz repletion rate. This count rate corresponds to photon generation rate of ~10 Mcps at the output of quantum Tx. This value is very close to the calculated value by taking into account the various practical parameters such as beam splitter efficiency (~50%), mean photon number (~10%), SPD efficiency (~70%), coupling efficiency (~90%) etc. The dark counts are measured to be <100 counts/sec/SPD.

## IV. Software Implementation of BB84 Protocol

The software code for overall system control and monitoring of our BB84 protocol based QKD testbed is developed using the NI LabVIEW platform. The classical communication required for public discussion is performed using a TCP/IP connection established between the two computers i.e. Alice and Bob PC over Intranet. The flow of software procedures for implementing the BB84 protocol based QKD between Alice and Bob is described as below:

### A. Qubit Exchange:

*Quantum Tx (Alice) setup:* The Software code for Tx side FPGA DIO module is optimized for generating 10 ns pulses (adjustable) at 10MHz repetition rate. To generate the trigger signal for laser diodes, two pseudorandom strings set of 0's and 1's are generated inside the Tx FPGA module. The first string is responsible for generating Alice's raw key bits and the second one is used to randomly select the polarization basis. Combined they form one of the four polarization state to be generated and thus the pulse laser module to be triggered.

Furthermore, intercept-and-retransmit type of Eve attack is also implemented in the Tx FPGA such that if Eve is present, the polarization state generated out of the quantum Tx hardware is encoded as per Eve's bases and bits. Finally, all the relevant parameters required for further post-processing are transferred into Tx FIFO.

*Quantum Rx (Bob) setup:* The Rx side FPGA DIO module first performs overall clock and frame synchronization followed by continuous sampling of all four DIO channels connected to the SPDs generating ~17ns TTL output pulse per detection event. This channel status information is used to deduce Bob's basis and bit as per Table I. Finally, all these measured parameters are transferred into Rx FIFO for further processing.

TABLE I. Bit & Basis encoding/ decoding at Quantum Tx and Rx

| Alice (quantum Tx) | | | Bob (quantum Rx) | | |
|---|---|---|---|---|---|
| Random Bit | Random Basis | Polarization state | Triggered DIO channel | Deduced Bit | Deduced Basis |
| 0 | 0 (⊕) | $\|0°\rangle$ | 1 | 1 | 1 |
| | 1 (⊗) | $\|+45°\rangle$ | 2 | 0 | 1 |
| 1 | 0 (⊕) | $\|90°\rangle$ | 3 | 1 | 0 |
| | 1 (⊗) | $\|-45°\rangle$ | 4 | 0 | 0 |

### B. Secure key generation:

The software processing steps needed to establish the final shared secure key are similar for Alice and Bob and can be divided into following steps:

*a) Raw key generation:* A pre-defined chunk of data is read from FIFO at respective Alice and Bob PC and bit unpacking is performed to form the raw key.

*b) Sifted key generation:* Sifted key is then formed through basis sharing over the public channel by discarding those bits where bases mismatch has occurred. Computation of QBER is then carried out; which if found above a specified threshold, Eavesdropper's presence is flagged and thus any further communication is aborted. Else, both the parties form the updated sifted key.

*c) Quantum key generation:* This sifted key is then used to perform key distillation procedure (as discussed in Sec. II(C)), consisting of error correction and privacy amplification steps to form the truly random final secure quantum key, Ks.

### C. Secure data communication:

Now that both the parties: Alice and Bob have got the same quantum cryptographic keys, they can use them to perform secure data communication over unsecure public channel (TCP/IP in our case). In our set-up an image/text file

is encrypted at Alice PC by bitwise OTP (one-time padding) method using the established quantum key Ks and transmitted to Bob PC. The Bob then uses its own quantum key to decrypt the image/text file and recovers the data.

## V. Results and Discussion

The experimental testbed for QKD system is shown in Fig.4. This setup is situated in a dark room lab to suppress the noise contribution due to ambient light. The Bob's setup is placed in a black-out enclosure to further suppress the stray light. After establishing free space quantum communication link between Alice and Bob, a set of several experimental runs were conducted iteratively for several hours. For every run, the sifted key and final secure key is recorded and QBER performance is evaluated.


Fig. 4. Experimental testbed for free-space QKD system

The indigenously developed pulse laser module consists of a pulse driver circuit along with a TEC (Thermo-electric cooler) controller. The pulse driver is required to control the laser drive current as per the input TTL signal and the TEC controller is required to provide the wavelength & power stabilization over a temperature range. It is capable of generating optical pulses at a repetition rate of up to 100 MHz with pulse width as narrow as 5 ns. If the mean photon no. per pulse is set as 0.1, this is capable of generating count rate of upto 10 Mcps The polarized single photon streams is generated by heavily attenuating the coherent laser pulses. In order to determine the quality of single photon source, second order correlation function or normalized intensity correlation $g^{(2)}[n]$ is computed by performing Hanbury-Brown-Twiss (HBT) experiment. The measured $g^{(2)}[0]$ value of ~0.98 shows that the developed source exhibit Poissonian characteristic with very good quality. The fully assembled mechanical package of PLM is shown in Fig.5.

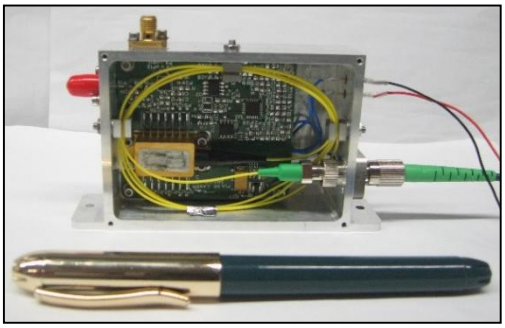

Fig. 5. Assembled pulse laser Module

The software code for BB84 QKD system on Tx and Rx side is optimized to operate at burst mode for quantum communication link and public link. The 1-s bursts are dedicated for quantum communication. The interval between these successive bursts, however, varies with the chunk size of FIFO data, processing capability and the available memory at Alice and Bob PC.

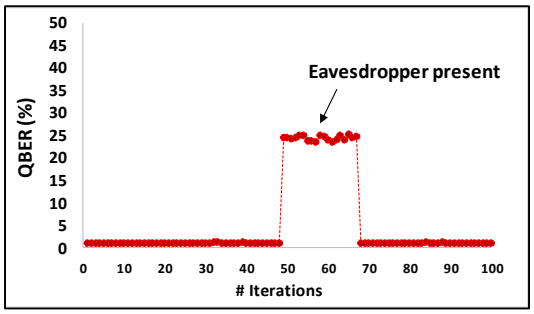


Fig. 6. Measured QBER for quantum free space link

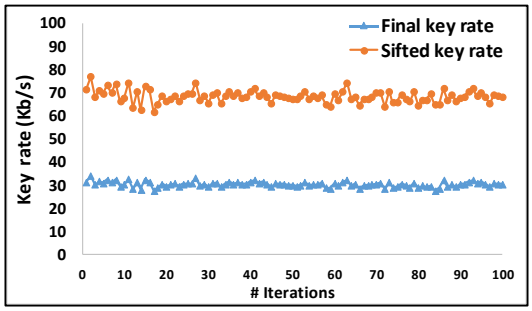


Fig. 7. Measured key rate (sifted & final) for quantum free space link

Fig.7 shows that in our QKD system, sifted key generation rate of ~70 kbps and final key rate of ~33 kbps is achieved for 10MHz pulse triggering. These key rates are calculated based on the execution timing of ~3.92s to complete the key sifting procedure and overall ~4.78s to establish the final secure key respectively. The final key rate is calculated after performing error correction and privacy amplification procedures for all the iterations wherever eavesdropper is found absent. For QBER computation, ~20% of the random bits are used out of the sifted key bits. The error correction scheme is implemented based on the Hamming algorithm. A privacy amplification procedure based on the Toeplitz matrix is implemented and key size is further reduced to ~70%. The experimental results with targeted specifications are tabulated in Table II.

TABLE II. Overall Summary of Measured Results

| Sr. | Parameters | Targeted Specs. | Measured Values |
|---|---|---|---|
| 1. | Wavelength | 785 nm | 784.36 nm |
| 2. | Pulse repetition rate | 10 MHz | 10 MHz |
| 3. | Pulse width | 10 ns | 10 ns |
| 4. | Polarization states @ Rx | $\|0°\rangle$, $\|90°\rangle$, $\|+45°\rangle$, $\|-45°\rangle$ | $\|0°\rangle$, $\|90°\rangle$, $\|+45°\rangle$, $\|-45°\rangle$ |
| 5. | Mean photon no. per pulse (μ) | ~0.1 | 0.11 |
| 6. | QBER | < 5% | ~1.2% |
| 7. | Sifted Key Rate | >50 Kbps | ~70 Kbps |
| 8. | Final key rate | >30kbps | ~33 kbps |

The measured QBER of <1.2% as shown in Fig.6 in the absence of eavesdropping can be attributed to imperfect devices. The experimental runs with eavesdropping attack resulted in QBER increased to ~25% when Eve is emulated to be present in the quantum channel link. This is very well in accordance with the theoretical results.

Furthermore, after the successful quantum key generation & distribution, an image file is encrypted using the quantum

key at Alice's PC and transmitted to Bob's PC over TCP/IP. This image data is decrypted using Bob's quantum key and image is then recovered perfectly in the absence of Eve. If however, for the sake of demonstration, the communication was continued even after detection of Eve i.e. with calculated QBER of ~25%, the final decrypted image is found completely unintelligible for any practical purposes, as can be seen in Fig.8. This way, the communication between Alice and Bob is demonstrated with unconditional security employing quantum cryptography.

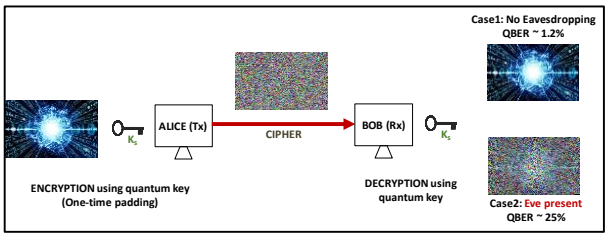


Fig. 8. Secure data transfer between Tx and Rx employing quantum key cryptography

## VI. CONCLUSION

We have reported successful implementation of the BB84 protocol and experimental demonstration of a fully automated QKD system employing weak coherent laser pulses. A pulse laser module was indigenously developed to generate narrow optical pulses with high repetition rate. A free space quantum communication link over a distance of ~ 2 m was established by exploiting the polarization encoded stream of single photons. The QKD system demonstrates a low QBER of ~1.2% with sifted key generation rate of ~70 Kbps at an average photon number per pulse $\mu$= 0.11 for pulse repetition rate of 10 MHz. The final secure key rate of ~33 Kbps was achieved after performing post processing procedures viz. error correction and privacy amplification. The performance of quantum communication link was continuously verified for several hours and found highly satisfactory. Our QKD system is shown to be capable of distributing cryptographic keys securely and seamlessly, under practical operating conditions. Finally, an unconditionally secure transmission of an image between Alice and Bob connected over an unsecured public channel is demonstrated by exploiting quantum cryptography.

In future, the pulse repetition rate of 10MHz would be further increased to enhance the key generation capacity. The overall execution time would also be reduced through further optimization of both the back-end and front-end software codes. We also plan to upgrade our QKD system to demonstrate secure communication between two buildings. Implementation of the more advanced QKD protocols such as decoy state BB84 protocol, which are more robust against eavesdropping attack and capable of achieving higher secure key rate are also in progress.

## ACKNOWLEDGMENT

The authors would like to acknowledge Shri. D K Das, Director, Space Applications Centre (SAC), Ahmedabad, Shri. N M Desai, Associate Director, SAC, Shri. K S Parikh, Deputy Director, SATCOM & Navigation Payload Area and Shri T V S Ram, Group Director, ODCG, for their encouragement and continuous support to this work.

## REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, pp. 175-179, 1984.

[2] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys*, vol. 74, pp 145-195, 2002.

[3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck et al., "Advances in quantum cryptography", *arXiv:1906.01645v1 [quant-ph]*, Jun 2019.

[4] A. K. Ekert, "Quantum cryptography based on Bell's theorem", *Phys. Rev. Lett*. 67, p. 661, 1991.

[5] C. H. Bennett, G. Brassard, N. D. Mermin, "Quantum cryptography without Bell's theorem", *Phys. Rev. Lett*. 68, p. 557, 1992.

[6] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl et al. , "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett*. 98(1), 2007.

[7] B. Korzh et al. "Provably Secure and Practical Quantum Key Distribution over 307 km of Optical Fibre". *Nature Photonics* 9, pp. 163-168, 2015.

[8] R. Bedington, J. M. Arrazola and A. Ling, "Progress in satellite quantum key distribution," *NPJ Quantum information*, vol. 3, Article no. 30, 2017.

[9] S.K. Liao et al., "Satellite-to-ground quantum key distribution," *Nature*, vol 549, pp 43-47 (2017)

[10] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, S. Masahide and M. Toyoshima, "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite," *Nature Photonics*, vol 9, pp. 502-508 (2017)

[11] J. S. Johnson, M.R. Grimaila, J.W. Humphries and G.B. Baumgartner, "An analysis of error reconciliation protocols used in Quantume Key Distribution Systems," *Journal of Defense Modelling and Simulation*, vol. 12, no. 3, pp. 217-227, 2015.

[12] M. Hayashi, "Exponential decreasing rate of leaked information in universal random privacy amplification," *IEEE Transactions on Information Theory* 57, pp. 3989–4001, 2011.